SPYWOLF

Security Audit Report

Completed on

July 5, 2023

OVERVIEW

This audit has been prepared for **Vanish** to review the main aspects of the project to help investors make make an informative decision during their research process.

You will find a a summarized review of the following key points:

- ✔ Contract's source code
- ✔ Owners' wallets
- ✔ Tokenomics
- ✔ Team transparency and goals
- ✔ Website's age, code, security and UX
- ✔ Whitepaper and roadmap
- ✔ Social media & online presence

The results of this audit are purely based on the team's evaluation and does not guarantee nor reflect the projects outcome and goal

- SPYWOLF Team -

TABLE OF CONTENTS

Vanish

PROJECT DESCRIPTION

According to their website:

The Vanish Transfer System (VTS) breaks Ethereum's Blockchain informational link between the source wallet and destination wallet when sending ERC-20 assets. This serves to provide anonymity to our users who desire to navigate the crypto space with full privacy.
You're just one transaction away... why not? Leave without a trace.

Release Date: Presale starts in July, 2023

Category: Crypto mixer

CONTRACT INFO

Token Name	Symbol
Vanish	$Vanish

Contract Address
0x6f4dde2ddf242a3b10cd3c50d0ad0fbf5ddf996b

Network	Language
Ethereum	Solidity

Deployment Date	Verified?
Jun 30, 2023	Yes

Total Supply	Status
1,000,000,000	Not launched

TAXES

Buy Tax
none

Sell Tax
none

*Taxes can be changed in future

Our Contract Review Process

The contract review process pays special attention to the following:

- Testing the smart contracts against both common and uncommon vulnerabilities
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Ensuring contract logic meets the specifications and intentions of the client.
- Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- Thorough line-by-line manual review of the entire codebase by industry experts.

Blockchain security tools used:

- OpenZeppelin
- Mythril
- Solidity Compiler
- Hardhat

TOKEN TRANSFERS STATS

Transfer Count	2
Uniq Senders	2
Uniq Receivers	2
Total Amount	2000000000 $Vanish
Median Transfer Amount	1000000000 $Vanish
Average Transfer Amount	1000000000 $Vanish
First transfer date	2023-06-30
Last transfer date	2023-07-03
Days token transferred	2

SMART CONTRACT STATS

Calls Count	3
External calls	3
Internal calls	0
Transactions count	3
Uniq Callers	1
Days contract called	2
Last transaction time	2023-07-03 20:56:59 UTC
Created	2023-06-30 22:38:23 UTC
Create TX	0x39194f5c2067lf8d310763a4908f3033d7c38384f4ed14883b2eecf9cd7d3a93
Creator	0x7a787ff7d51c742c7173318e2f93a787810d0554

VULNERABILITY CHECK

Design Logic	Passed
Compiler warnings.	Passed
Private user data leaks	Passed
Timestamp dependence	Passed
Integer overflow and underflow	Passed
Race conditions and reentrancy. Cross-function race conditions	Passed
Possible delays in data delivery	Passed
Oracle calls	Passed
Front running	Passed
DoS with Revert	Passed
DoS with block gas limit	Passed
Methods execution permissions	Passed
Economy model	Passed
Impact of the exchange rate on the logic	Passed
Malicious Event log	Passed
Scoping and declarations	Passed
Uninitialized storage pointers	Passed
Arithmetic accuracy	Passed
Cross-function race conditions	Passed
Safe Zeppelin module	Passed
Fallback function security	Passed

THREAT LEVELS

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and access control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time. We categorize these vulnerabilities by the following levels:

High Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Medium Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Low Risk

Issues on this level are minor details and warning that can remain unfixed.

Informational

Information level is to offer suggestions for improvement of efficacy or security for features with a risk free factor.

FOUND THREATS

⚠ Medium Risk

If there are enough tokens accumulated for auto swap and auto swap is enabled and taxes are set to 0, totalETHFee's value will become zero (0) and contract will halt on sell.
Division by zero (0) is impossible.

```
function _transfer(address sender, address recipient, uint256 amount) private returns (bool) {
.................................
uint256 contractTokenBalance = balanceOf(address(this));
bool overMinimumTokenBalance = contractTokenBalance >= minimumTokensBeforeSwap;

if (overMinimumTokenBalance && !inSwapAndLiquify && !isMarketPair[sender] && swapAndLiquifyEnabled)
{
    if(swapAndLiquifyByLimitOnly)
        contractTokenBalance = minimumTokensBeforeSwap;
    swapAndLiquify(contractTokenBalance);
}
.................................
}

function swapAndLiquify(uint256 tAmount) private lockTheSwap {
.................................
    uint256 totalShares = _totalTaxIfBuying.add(_totalTaxIfSelling);
    uint256 totalETHFee = totalShares.sub(liquidityShare.div(2));

    uint256 amountETHLiquidity = recievedBalance.mul(liquidityShare).div(totalETHFee).div(2);
    uint256 amountETHMarketing = recievedBalance.mul(MarketingShare).div(totalETHFee);
    uint256 amountETHDeveloper = recievedBalance.sub(amountETHLiquidity).sub(amountETHMarketing);
.................................
}
```

- Recommendation:
  - Ensure that division by zero (0) won't occur

FOUND THREATS

⚠ Low Risk

Owner can change current router.
If set to inappropriate router, contract might halt on sell.

```
function changeRouterVersion(address newRouterAddress) public onlyOwner returns(address newPairAddress) {

    IUniswapV2Router02 _uniswapV2Router = IUniswapV2Router02(newRouterAddress);

    newPairAddress = IUniswapV2Factory(_uniswapV2Router.factory()).getPair(address(this), _uniswapV2Router.WETH());

    if(newPairAddress == address(0)) //Create If Doesnt exist
    {
        newPairAddress = IUniswapV2Factory(_uniswapV2Router.factory())
            .createPair(address(this), _uniswapV2Router.WETH());
    }

    uniswapPair = newPairAddress; //Set new pair address
    uniswapV2Router = _uniswapV2Router; //Set new router address

    isMarketPair[address(uniswapPair)] = true;
}
```

- Recommendation:
  - Router change is not recommended after token's launch.

Informational

Owner can withdraw any tokens from the contract except the native $Vanish token.
When this function is present, in cases tokens sent into the contract by mistake or purposefully, contract's owner can retrieve them.

```
function rescueStuckToken(address _token, uint _amount) external onlyOwner {
    require(_token != address(this), "Owner can't claim contract's balance of its own tokens");
    IERC20(_token).transfer(msg.sender,_amount);
}

function rescueFunds() external onlyOwner {
    (bool os,) = payable(msg.sender).call{value: address(this).balance}("");
    require(os);
}
```

Owner can set buy/sell fees up to 12.5%.
Combined buy+sell = 25%.
When fees are above 0, there will be certain amount of tokens that will be deducted from every transaction that users make.
Deducted amount will be as much as the fees % from total amount that user had bought, sold and/or transferred.

```
function setBuyTaxes(uint _Liquidity, uint _Marketing , uint _Developer) public onlyOwner {
    _buyLiquidityFee = _Liquidity;
    _buyMarketingFee = _Marketing;
    _buyDeveloperFee = _Developer;
    _totalTaxIfBuying = _buyLiquidityFee.add(_buyMarketingFee).add(_buyDeveloperFee);
    require(_totalTaxIfBuying <= (feeUnits/8), "Buy fees must be 12.5% or less");
}

function setSellTaxes(uint _Liquidity, uint _Marketing , uint _Developer) public onlyOwner {
    _sellLiquidityFee = _Liquidity;
    _sellMarketingFee = _Marketing;
    _sellDeveloperFee = _Developer;
    _totalTaxIfSelling = _sellLiquidityFee.add(_sellMarketingFee).add(_sellDeveloperFee);
    require(_totalTaxIfSelling <= (feeUnits/8), "Sell fees must be 12.5% or less");
}
```

Informational

Owner can exclude address from fees.
When address is excluded from fees, the user will receive the whole amount of the bought, sold and/or transferred tokens.

```
function setIsExcludedFromFee(address account, bool newValue) public onlyOwner {
    isExcludedFromFee[account] = newValue;
}
```

Owner can exclude address from max transaction and max wallet limit.

```
function setIsTxLimitExempt(address holder, bool exempt) external onlyOwner {
    isTxLimitExempt[holder] = exempt;
}

function setIsWalletLimitExempt(address holder, bool exempt) external onlyOwner {
    isWalletLimitExempt[holder] = exempt;
}
```

Owner can set max transaction limit but cannot lower it than 0.1% of total supply.

```
function setMaxTxAmount(uint256 maxTxAmount) external onlyOwner() {
    require(maxTxAmount >= _totalSupply.mul(1).div(1000),
    "Cannot set max TX amount lower than 0,1% of total supply");
    _maxTxAmount = maxTxAmount;
}
```

RECOMMENDATIONS FOR

GOOD PRACTICES

1. Consider fundamental tradeoffs
2. Be attentive to blockchain properties
3. Ensure careful rollouts
4. Keep contracts simple
5. Stay up to date and track development

Vanish

GOOD PRACTICES FOUND

- ✔ The owner cannot mint new tokens after deployment
- ✔ The owner can set a transaction limit, but can’t lower it than 0.1% of total supply
- ✔ The smart contract utilizes "SafeMath" to prevent overflows

There is no information about the initial tokens distribution based on the project's whitepaper and/or website.

TOKENOMICS

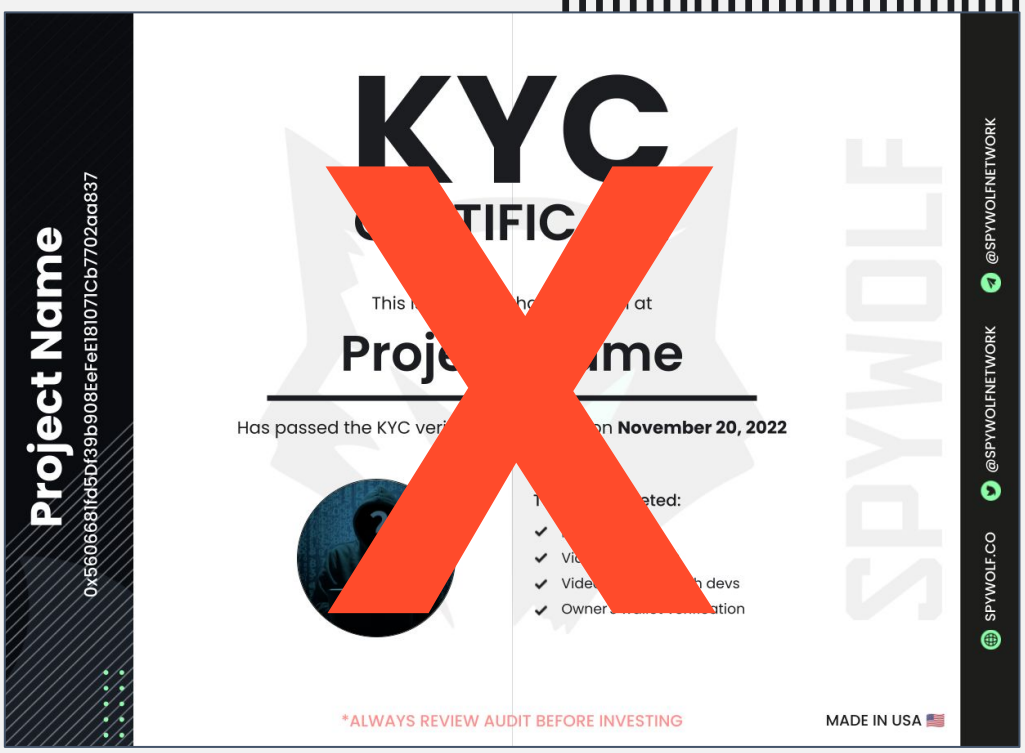
THE TEAM

⚠️ The team is annonymous

KYC INFORMATION

No KYC

We recommend the team to get a KYC in order to ensure trust and transparency within the community.



WEBSITE

Website URL
https://vanisheth.com/

Domain Registry
https://www.godaddy.com

Domain Expiration
Expires on 2024-06-19

Technical SEO Test
Passed

Security Test
Passed. SSL certificate present

Design
Single page design with appropriate color scheme and graphics.

Content
The information helps new investors understand what the product does right away. No grammar mistakes found.

Whitepaper
Well written, explanatory.

Roadmap
Yes, goals set without time frames.

Mobile-friendly?
Yes

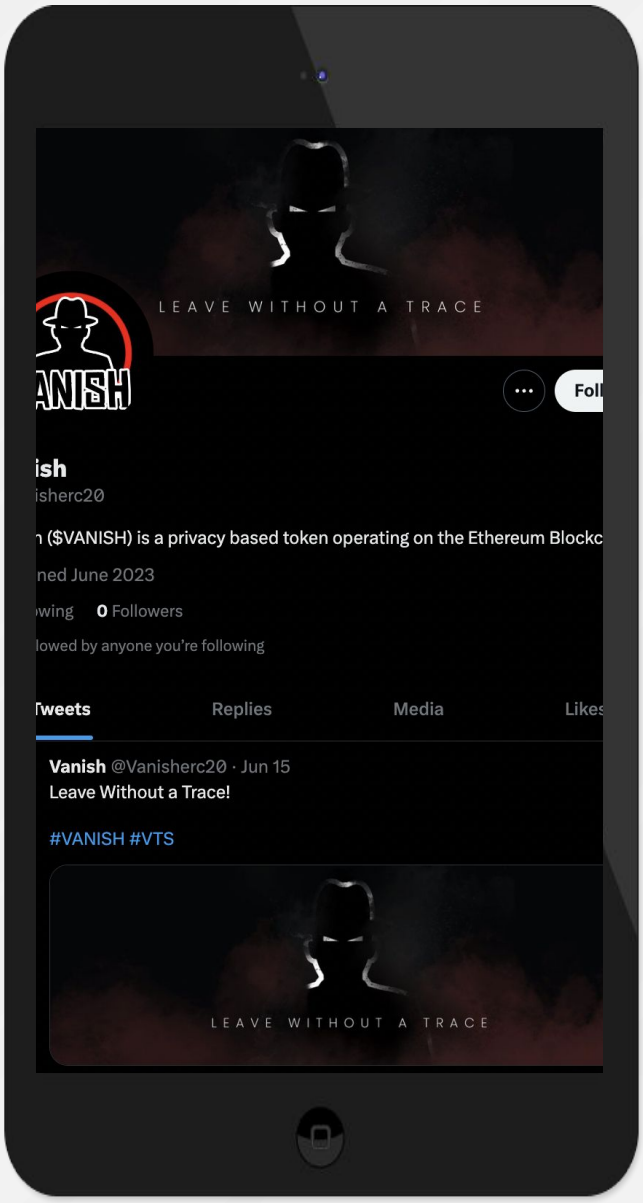
vanisheth.com

SOCIAL MEDIA

& ONLINE PRESENCE

ANALYSIS

Project's social media pages are new



Twitter

@vanisherc20

- No followers
- 1 post
- New account

Discord

- Not available

Telegram

@Vanish_Portal

- 12 members
- 1 post
- Announcement channel

Medium

- Not available

SPYWOLF

CRYPTO SECURITY

Audits | KYCs | dApps
Contract Development

ABOUT US

We are a growing crypto security agency offering audits, KYCs and consulting services for some of the top names in the crypto industry.

- **OVER 500 SUCCESSFUL CLIENTS**
- **MORE THAN 500 SCAMS EXPOSED**
- **MILLIONS SAVED IN POTENTIAL FRAUD**
- **PARTNERSHIPS WITH TOP LAUNCHPADS, INFLUENCERS AND CRYPTO PROJECTS**
- **CONSTANTLY BUILDING TOOLS TO HELP INVESTORS DO BETTER RESEARCH**

To hire us, reach out to
contact@spywolf.co or
t.me/joe_SpyWolf

FIND US ONLINE

SPYWOLF.CO

@SPYWOLFNETWORK

@SPYWOLFNETWORK

Disclaimer

This report shows findings based on our limited project analysis, following good industry practice from the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, overall social media and website presence and team transparency details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report.
While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

DISCLAIMER:
By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice.
No one shall have any right to rely on the report or its contents, and SpyWolf and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (SpyWolf) owe no duty of care towards you or any other person, nor does SpyWolf make any warranty or representation to any person on the accuracy or completeness of the report.
The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and SpyWolf hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, SpyWolf hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against SpyWolf, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts, website, social media and team.
No applications were reviewed for security. No product code has been reviewed.